勒索軟體辨識與解密工具

Version 1.0

2021 年 7 月 9 日

TLP: WHITE

1. 簡介

加密勒索軟體 Ransomware 為一種透過資料加密手法讓受害者失去資料存取或系統的控制的惡意程式，且如不支付贖金給犯罪組織，則將無法取回受加密的資料。因犯罪組織利用這種不法模式獲利，也是其被稱為「勒索軟體」的原因。

現今的勒索軟體精密複雜且侵入性強大，透過發展各種攻擊手段與支援多國語言、跨平台等方式感染受害者設備。目前防毒軟體廠商對於部分勒索軟體已有可應對的免費解密工具，如不慎受到勒索軟體攻擊，可先參考本篇第二章節，辨識勒索軟體名稱後，透過第三章節的解密工具清單，搜尋是否有可支援的解密工具。

2. 勒索病毒種類辨識

勒索軟體種類眾多，為了取得對應的解密工具，需先正確地辨識勒索軟體名稱。本篇提供以下線上勒索軟體辨識服務，可透過提供‘勒索內容’(如: 勒索訊息、勒索電子郵件、網站網址等)與‘被加密的檔案’進行特徵比對，判定勒索軟體名稱。

1. **ID Ransomware**
   由 MalwareHunterTeam 提供，可辨識超過 1000 種勒索軟體。使用者可透過上傳加密檔案、勒索訊息(如無勒索訊息，可提供勒索電子郵件、網站網址)，即可進行辨識。網頁上傳介面如圖 1 所示。勒索軟體名稱辨識結果示意圖如圖 2 紅框處所示。
   網址請參考:
   ID Ransomware 官網: https://id-ransomware.malwarehunterteam.com/index.php

圖 1、ID Ransomware 上傳頁面

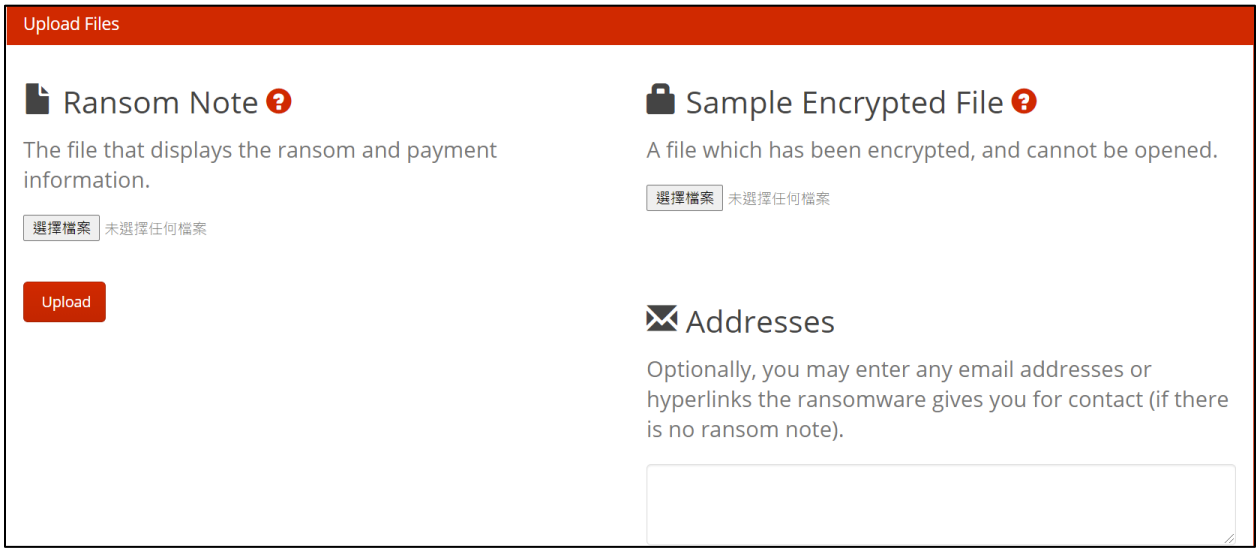


圖 2、ID Ransomware 勒索軟體名稱的辨識結果示意圖(紅框處)

2. **Crypto Sheriff**

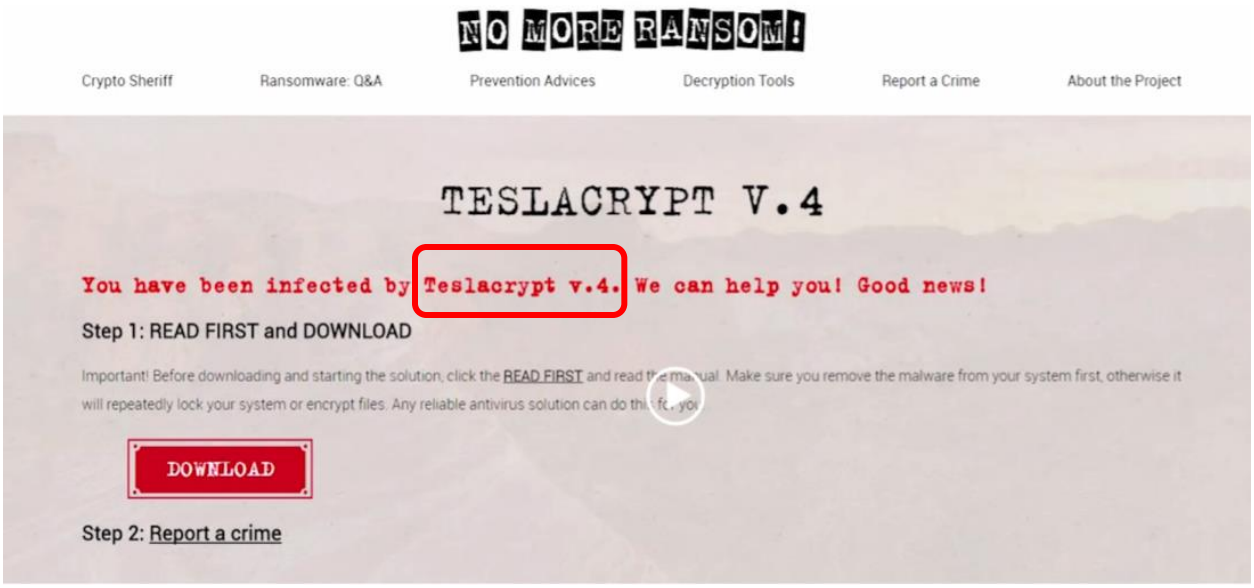
由 The No More Ransom Project 提供，可辨識勒索病毒並提供對應的免費解密工具。使用者可透過上傳兩個加密檔案、上傳勒索訊息檔案或是提供勒索訊息內容的電子郵件、網站網址、洋蔥網路網址、比特幣網址，即可進行辨識。上傳網頁介面如圖 3 所示。結果示意圖如圖 4 所示。

網址請參考:

No More Ransom 官網: https://www.nomoreransom.org/crypto-sheriff.php?lang=zht_Hant

圖 3、No More Ransom 解碼警長頁面

圖 4、解碼警長勒索軟體名稱辨識結果示意圖 (紅框處)



3. 解密工具

勒索軟體名稱確認之後，可透過本章節所提供之解鎖工具網頁清單，搜尋勒索軟體名稱或是瀏覽解密工具清單找到對應的解密工具，少數勒索軟體有機會使用以下工具嘗試解密。勒索軟體名稱辨識方式請參考本篇第二章節。

1. **No More Ransom 解鎖工具**
   由 No More Ransom Project 提供。使用者可透過搜尋勒索軟體名稱(紅框處)或是瀏覽解鎖工具列表(藍框處) (圖 5) ，查看工具使用指南與下載(圖 6) 。
   網址請參考:
   No More Ransom 官網: https://www.nomoreransom.org/zht_Hant/decryption-tools.html

圖 5、No More Ransom 解鎖工具列表與搜尋頁面

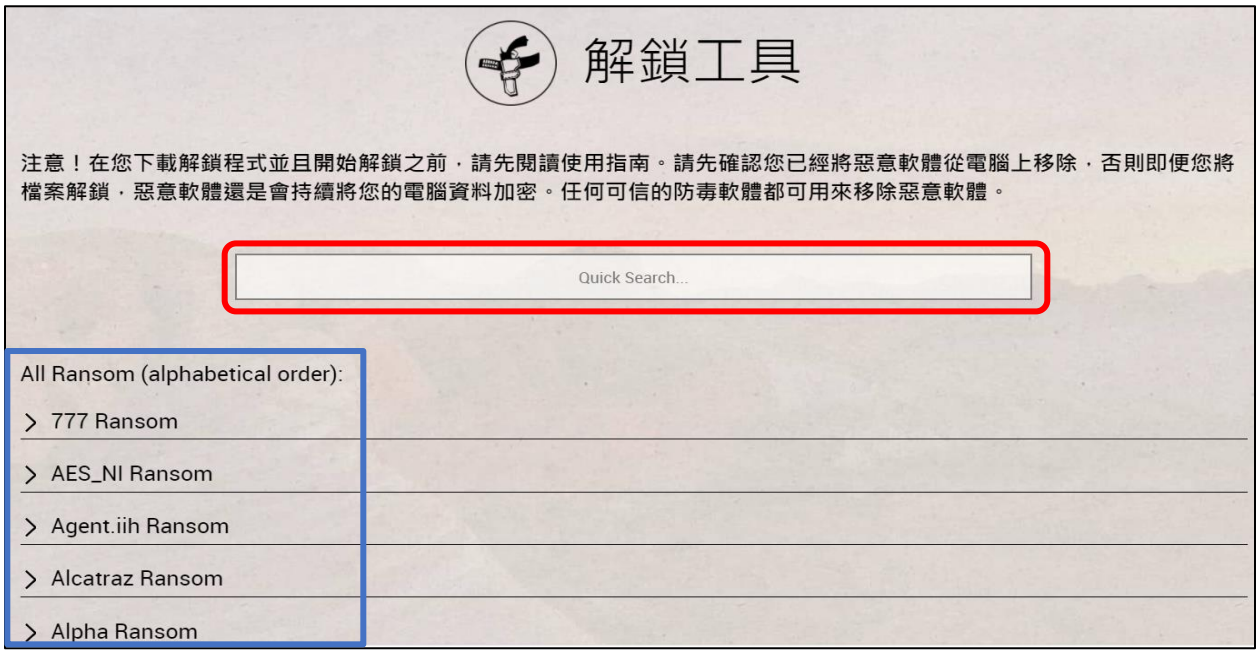
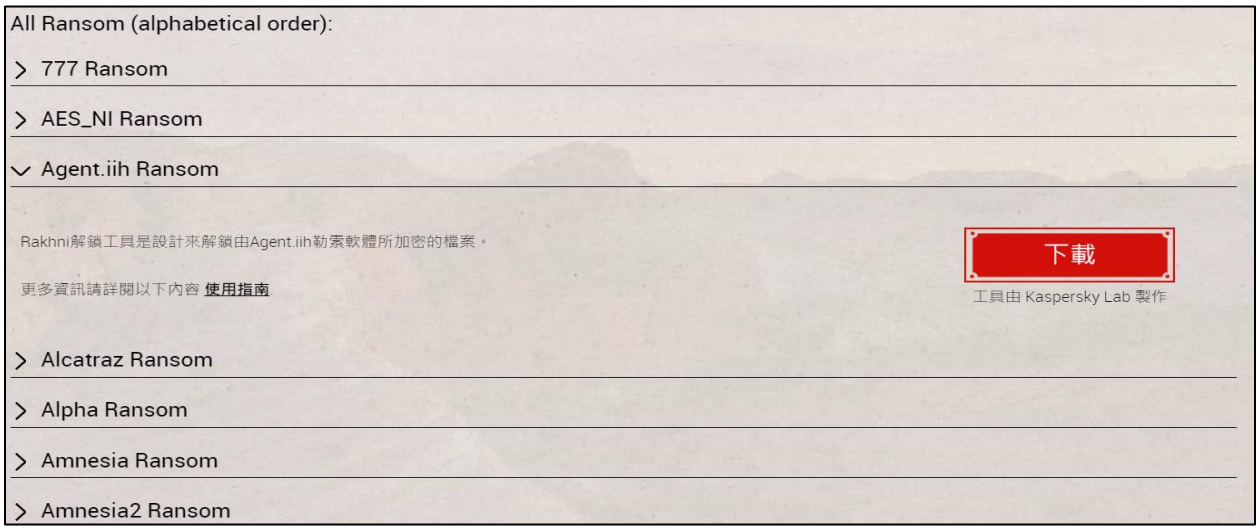
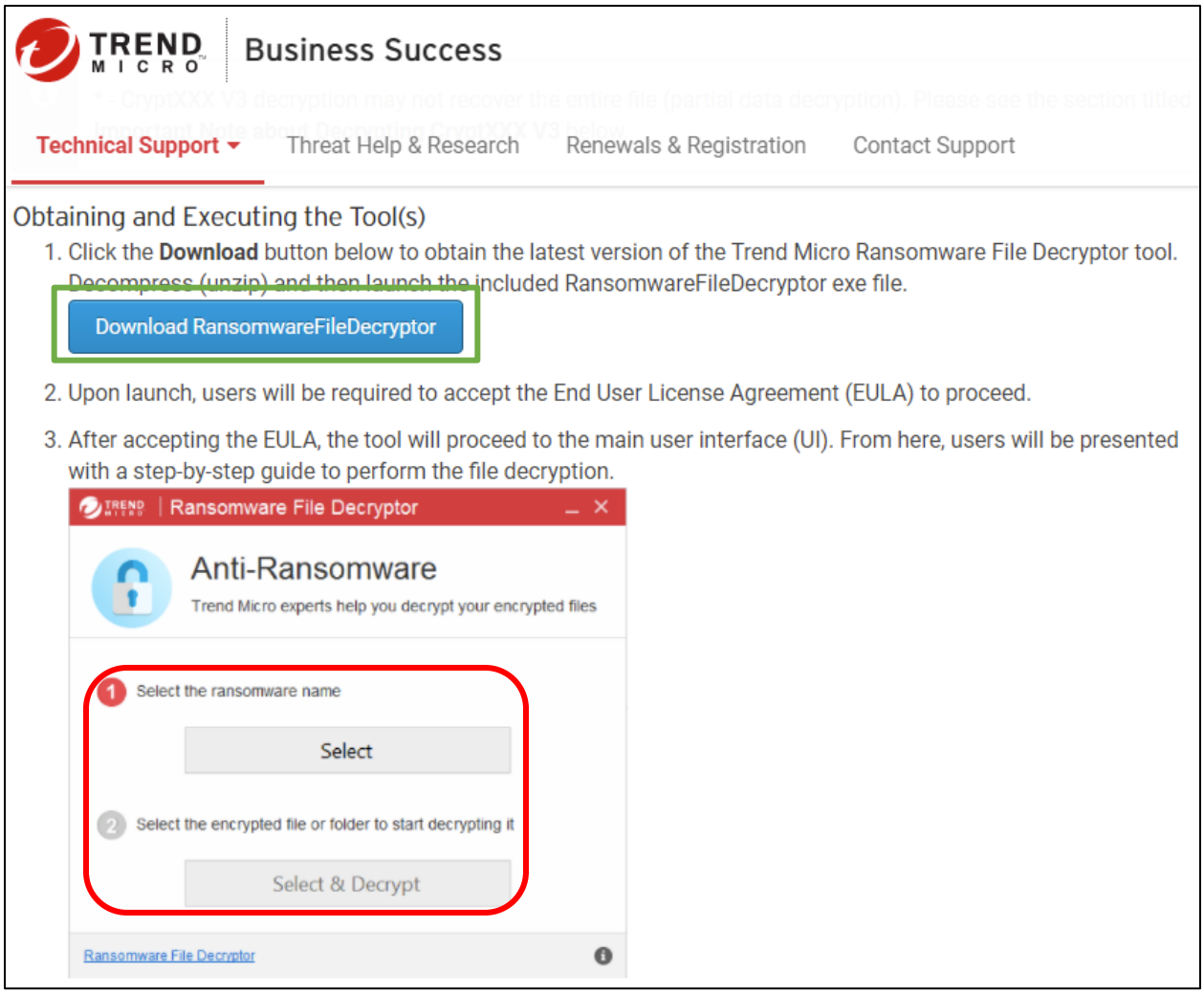


圖 6、No More Ransom 解鎖工具之說明、使用指南與工具下載連結頁面



2. **Trend Micro Ransomware File Decryptor**
   由 Trend Micro 提供。使用者可下載 (綠框處)與執行 RansomwareFileDecryptor 工具，選擇勒索軟體名稱與欲解密的檔案或資料夾進行解密(紅框處)。頁面如圖 7 所示。
   網址請參考:
   Trend Micro 官網: https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

圖 7、Trend Micro Ransomware File Decryptor 下載與說明頁面



3. **卡巴斯基 Free Ransomware Decryptors**

由卡巴斯基提供。使用者可瀏覽解密工具列(藍框處)表或是搜尋名稱(紅框處)，下載所需之解密工具進行解密。搜尋畫面與列表如圖 8 所示。

網址請參考:

卡巴斯基官網: https://noransom.kaspersky.com/

圖 8、卡巴斯基 Free Ransomware Decryptor 解密工具搜尋與瀏覽頁面

4. AVG 免費軟體解密工具

由 AVG 提供。使用者可瀏覽解密工具列表(圖 9)(藍框處)，檢視解密工具說明與下載修正程式進行解密(圖 10)。

網址請參考:

AVG 官網: https://www.avg.com/zh-tw/ransomware-decryption-tools

圖 9、AVG 免費勒索軟體解密工具列表頁面

圖 10、工具說明、勒索訊息畫面與修正程式下載連結 (示意圖)

5. **EMSI SOFT Free Ransomware Decryption Tools**
   由 EMSI SOFT 提供。使用者可瀏覽解密工具列表(藍框處)，下載所需解密工具(圖 11)。
   網址請參考:
   EMISI SOFT 官網: https://www.emsisoft.com/ransomware-decryption-tools/free-download

圖 11、EMISI SOFT Free Ransomware Decryption Tool 解密工具列表頁面

6. **McAfee Ransomware Recover (Mr²)**
   Mr² 為 McAfee 開發之解密工具，採取指令列介面，且定期更新支援的勒索軟體主類。使用者可透過圖 12 下載安裝 Mr² (綠框處)，執行後可透過指令檢視支援解密的勒索軟體列表與進行解密，如圖 13 所示。

   網址請參考:
   McAfee 官網: https://www.mcafee.com/enterprise/zh-tw/downloads/free-tools/ransomware-decryption.html

   使用 Mr2 破解勒索軟體 Stampado 之範例與說明:
   Stampado 勒索訊息如圖 14 所示，內容提示受害者需透過攻擊者電子郵件 (圖 14 紅框處)聯繫以取得解鎖碼輸入(圖 14 綠框處)進行檔案解密。
   1) 啟動 Mr2 後，輸入 'MfeDecrypt -list'指令(圖 15 綠框處)搜尋 'Stampado' 勒索軟體的解密工具(圖 15 紅框處)
   2) 執行 'MfeDecrypt -get stampado -ver 1.0.0'指令下載 Stampado 解密工具。(圖 16 紅框處)
   3) 執行 'MfeDecrypt -about stampado -ver 1.0.0'指令查看解密工具使用方式(圖 17 紅框處)。
   4) 透過 'MfeDecrypt -run stampado -ver 1.0.0 -args "-e FileUnlocker64@mail2tor.com'命令執行解密工具(圖 18 紅框處)，提供圖 14 紅框處的勒索聯絡電子郵件，取得解鎖碼(圖 18 綠框處)，並於圖 13 的勒索訊息畫面輸入解鎖碼進行檔案解密。

圖 12、McAfee Ransomware Recover (Mr2) 下載頁面

圖 13、Mr2 執行畫面，包含工具指令與說明

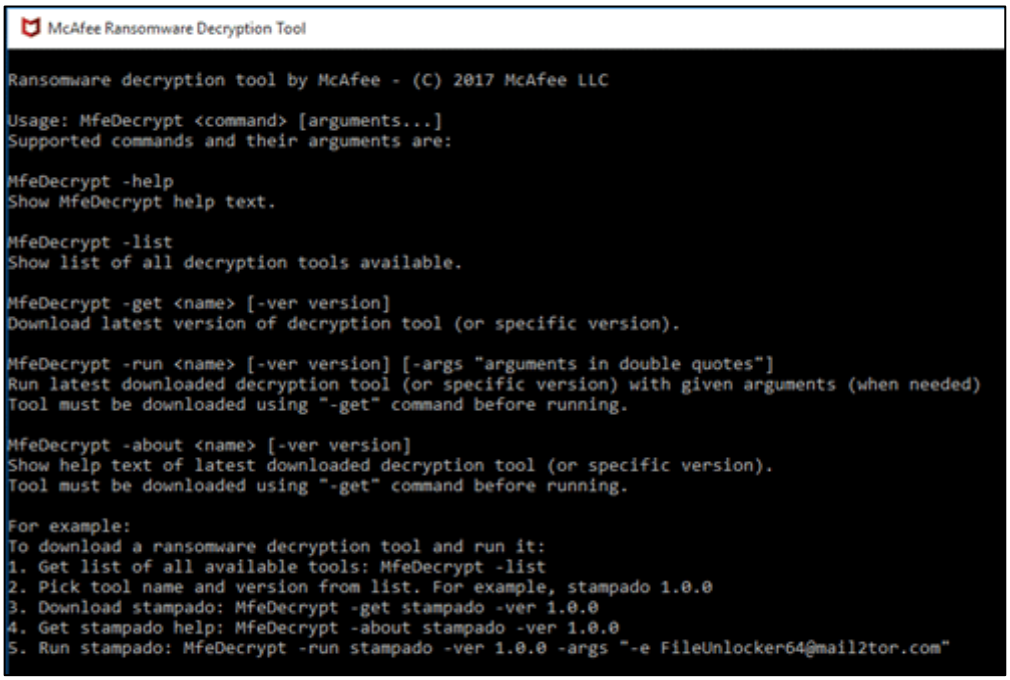


圖 14、Stampado 勒索訊息 (示意圖)

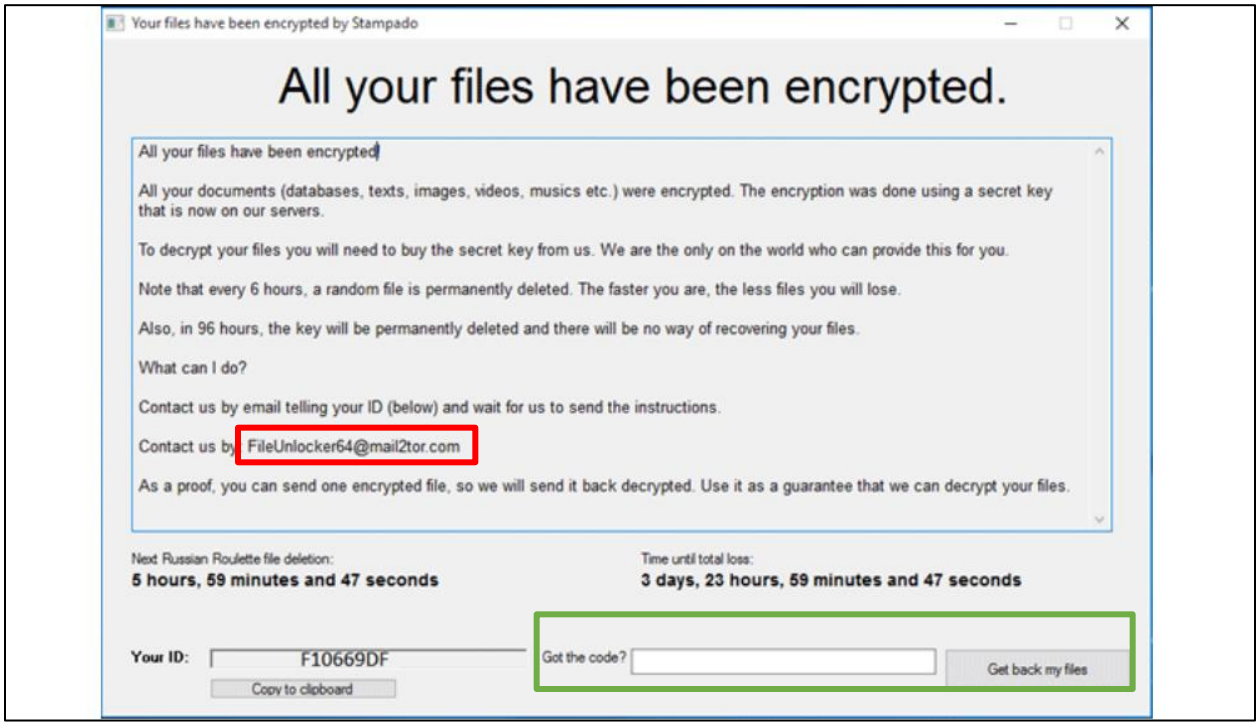


圖 15、Mr2 支援 Stampado 解密與顯示所有勒索軟體解密支援的命令 (示意圖)

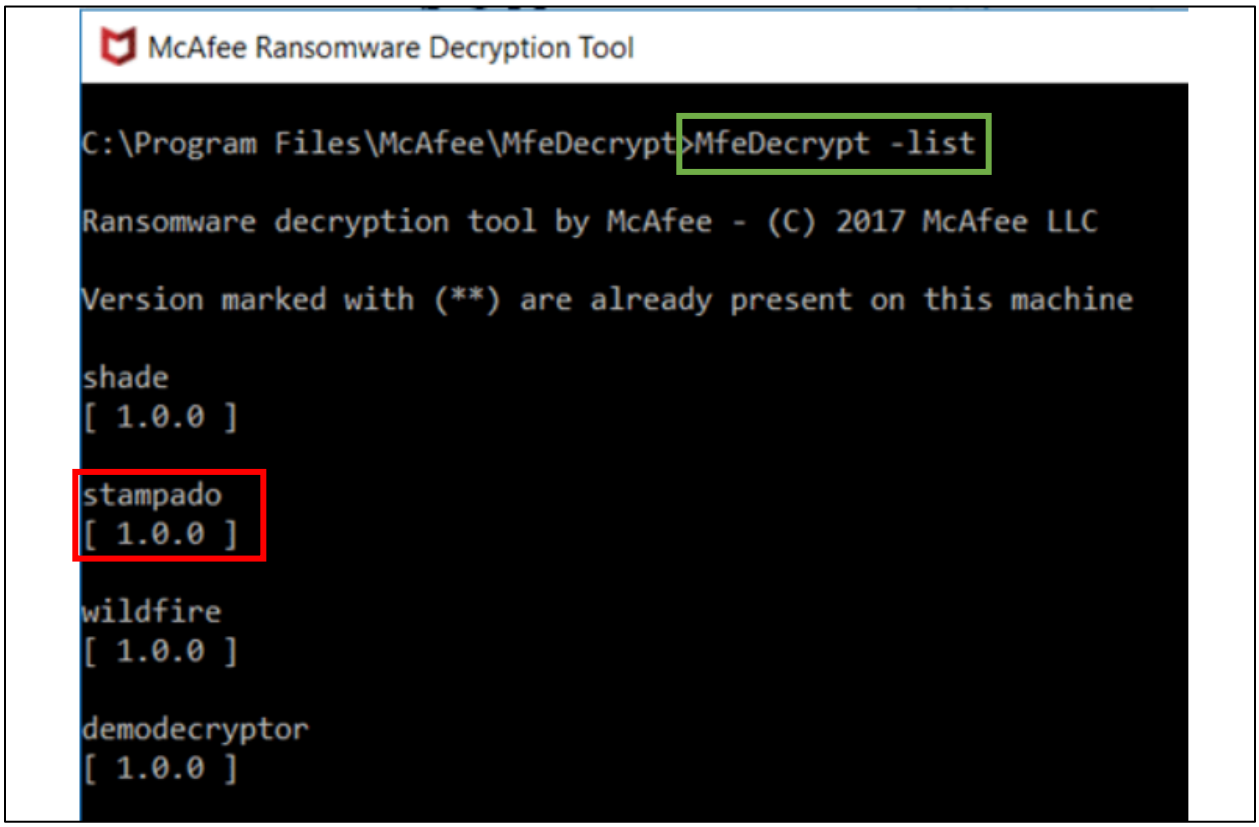


圖 16、下載勒索軟體 Stampado 解密工具的命令 (示意圖)

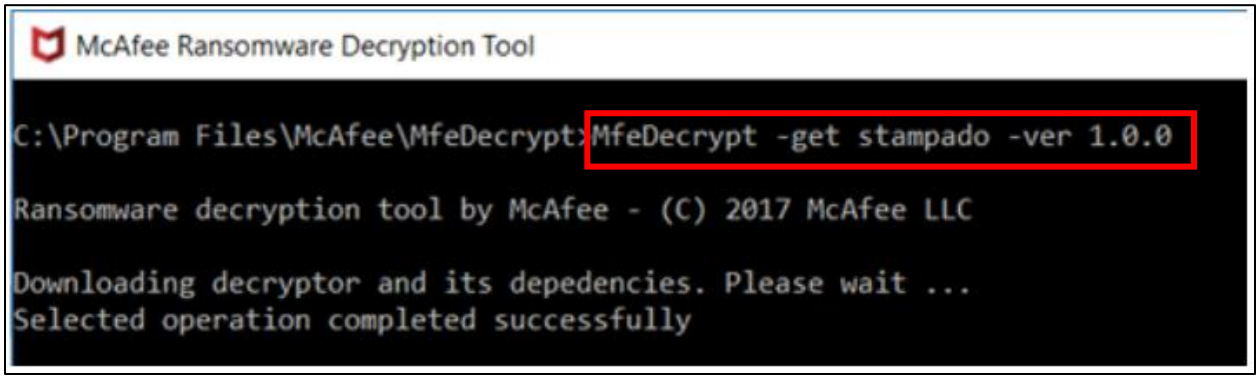


圖 17、Stampado 解密工具命令使用方式 (示意圖)

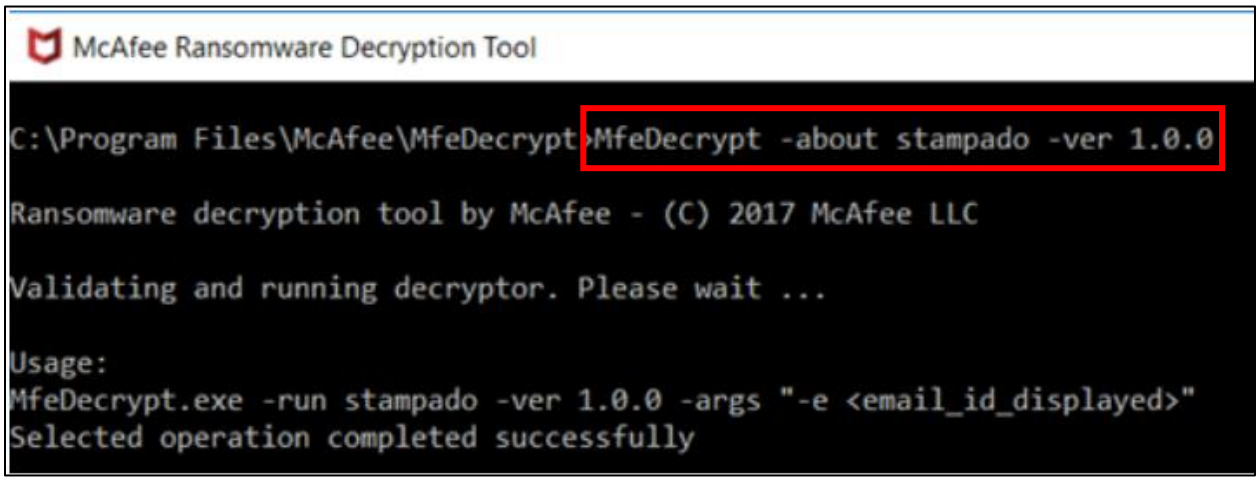
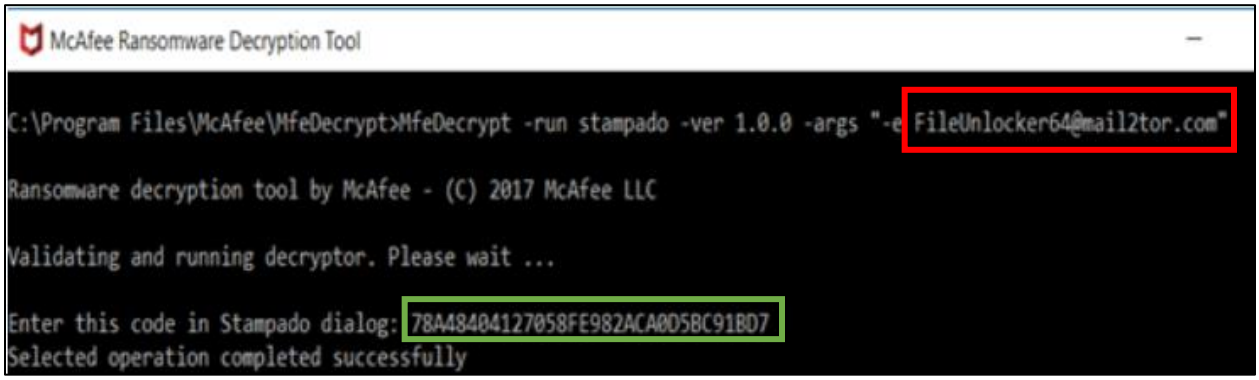


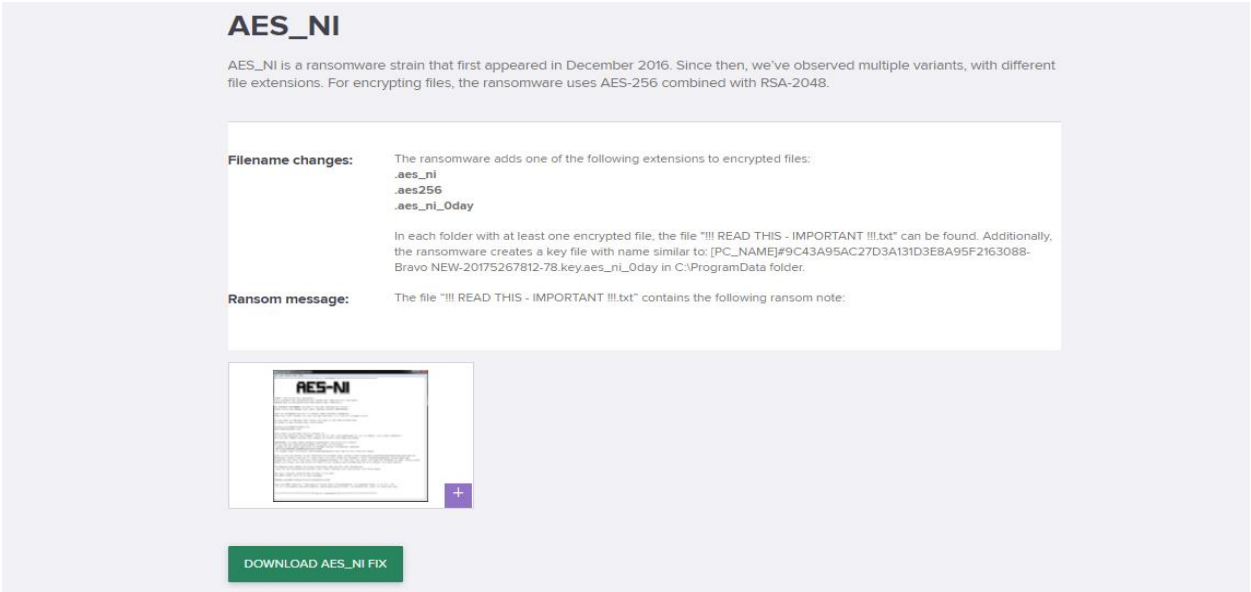
圖 18、取得 Stampado 解鎖碼 (示意圖)



7. **Avast Free Ransomware Decryption Tools**
   由 Avast 提供。使用者可瀏覽解密工具列表(圖 19) (藍框處)，檢視解密工具說明與下載修正程式進行解密(圖 20)。
   網址請參考:
   Avast 官網: https://www.avast.com/ransomware-decryption-tools

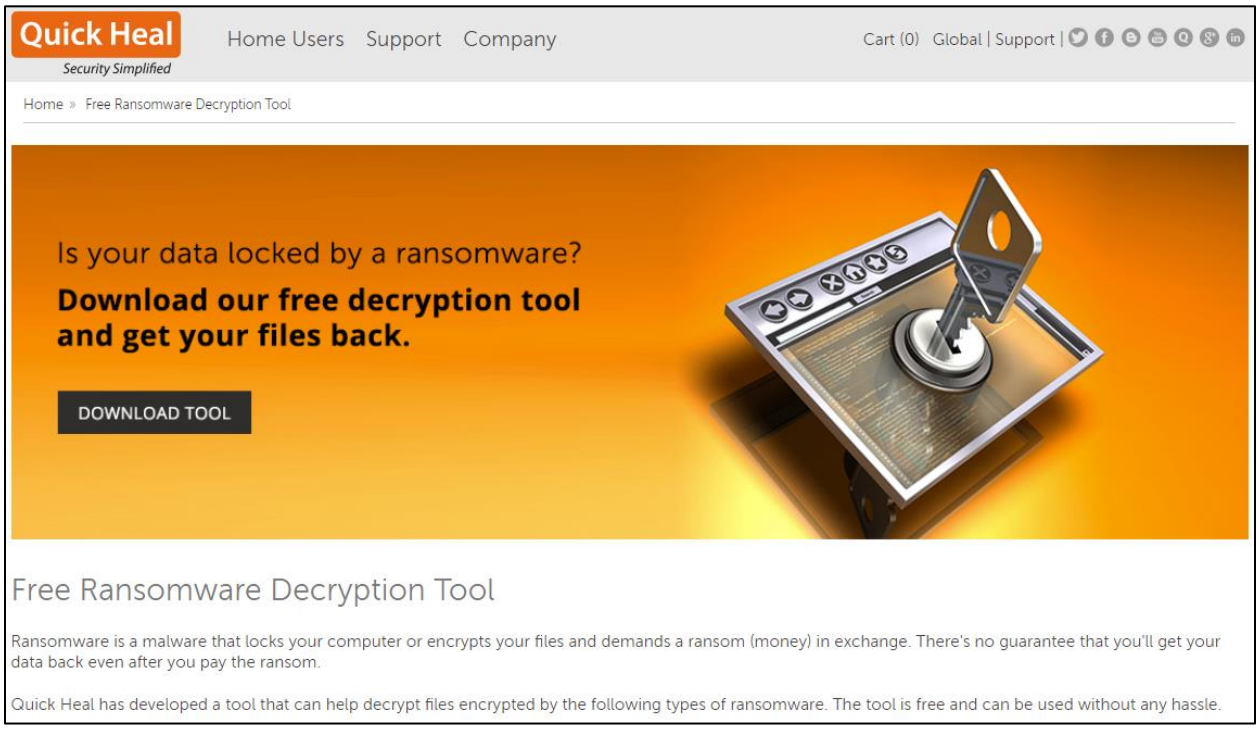
圖 19、Avast Free Ransomware Decryption Tool 解碼工具列表頁面

圖 20、解密工具說明、勒索訊息截圖與下載連結 (示意圖)



8. **Quick Heal Free Decryption Tool**
   由 Quick Heal 提供。使用者可下載支援多種勒索軟體解密的工具進行解密(圖21)。執行工具後，會自動進行掃描加密檔案進行解密。
   網址請參考:
   Quick Heal 官網: https://www.quickheal.com/free-ransomware-decryption-tool/

圖 21、Quick Heal Free Ransomware Decryption Tool 解密工具下載頁面



9. **MDS Ransomware Decryption Tools**
   由 MDR 提供。使用者可瀏覽解密工具列表，下載所需解密工具進行解密，如圖 22 所示。
   網址請參考:
   MDS 官網: https://www.mdsny.com/decryption-tools/

圖 22、MDS Ransomware Decryption Tools 解密工具列表